Billing Code: 7515-01U

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

[NARA-2018-062]

Privacy Act of 1974; System of Records

AGENCY: National Archives and Records Administration (NARA).

ACTION: Notice of a new system of records.

SUMMARY: The National Archives and Records Administration (NARA) proposes to add a system of records to its existing inventory of systems subject to the Privacy Act of 1974. In this notice, we publish NARA 45, Insider Threat Program Records. In addition, we are updating and republishing Appendix B to add the SORN's system manager and update other system manager contact information in the list of system managers and their addresses that apply to all NARA SORNs.

DATES: Submit comments on this system of records by **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].** This new system of records, NARA 45, and the Appendix B update, are applicable **[INSERT DATE 40 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** unless we receive comments that necessitate revising the SORN.

ADDRESSES: You may submit comments, identified by "SORN NARA 45," by one of the following methods:

- Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

- Email: Regulation_comments@nara.gov. Include SORN NARA 45 in the subject line of the message.
- Mail (for paper, disk, or CD-ROM submissions. Include SORN NARA 45 on the submission): Regulations Comment Desk, Strategy and Performance Division (MP), Suite 4100; National Archives and Records Administration; 8601 Adelphi Road; College Park, MD 20740-6001

Instructions: All submissions must include SORN NARA 45. We may publish any comments we receive without changes, including any personal information you include.

FOR FURTHER INFORMATION CONTACT: For more information on this SORN, contact Kimberly Keravuori, External Policy Program Manager, by email at regulation_comments@nara.gov, or by telephone at 301-837-3151. For information on the Insider Threat Program, contact Neil Carmichael, Insider Threat Program Director, by mail at National Archives and Records Administration; 8601 Adelphi Road; College Park, MD 20740-6001, or by telephone at 301-837-3169.

SUPPLEMENTARY INFORMATION:

We are establishing this system to implement the requirements of Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (October 7, 2011), and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (November 21, 2012).

For purposes of this system of records, the term "insider threat" is defined in the Minimum Standards for Executive Branch Insider Threat Programs, which were issued by the National Insider Threat Task Force based on directions provided in Section 6.3(b) of Executive Order 13587.

Our authorized insider threat program personnel use this system to maintain records that reflect and support the program's mission to detect, deter, and mitigate intentional or unintentional insider threats. This system will be part of a centralized hub for insider threat analysis and we will use it to manually and electronically gather, integrate, review, assess, analyze, audit, and respond to information derived from internal and external sources so we can mitigate threats that insiders may pose to NARA installations, facilities, personnel, missions, or resources. The system supports the NARA insider threat program, enables us to identify systemic insider threat issues and challenges, and provides a basis for developing and recommending solutions to mitigate potential insider threats.

The notice for this system of records states the record system's name and location, authority for and manner of operation, categories of individuals it covers, types of records it contains, sources of information in the records, and the "routine uses" for which the agency may use the information. The notice revising Appendix B includes the business address of NARA officials you may contact to find out how you may access and correct records pertaining to yourself.

The Privacy Act of 1974, as amended (5 U.S.C. 552(a)) ("Privacy Act"), provides certain safeguards for an individual against an invasion of personal privacy. It requires Federal agencies that disseminate any record of personally identifiable information to do so in a manner that assures the action is for a necessary and lawful purpose, the information is current and accurate for its intended use, and the agency provides adequate safeguards to prevent misuse of such information. NARA intends to follow these principles when transferring information to another agency or individual as a "routine use," including assuring that the information is relevant for the purposes for which it is transferred.

David S. Ferriero,

Archivist of the United States.

NARA 45

SYSTEM NAME AND NUMBER:

Insider Threat Program Records, NARA 45

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

The Office of the Chief Operating Officer at the National Archives in College Park maintains insider threat program records. The system address is the same as the system manager address.

SYSTEM MANAGER:

The system manager for insider threat program records is the Chief Operating Officer. The business addresses for system managers are listed in Appendix B, republished **[INSERT DATE OF PUBLICATION IN FEDERAL REGISTER]**. As system manager contact information is subject to change, for the most up-to-date information visit our website at www.archives.gov/privacy/inventory.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

44 U.S.C. 2104(a), as amended;

44 U.S.C. 3554, Federal agency responsibilities;

44 U.S.C. 3557, National security systems;

Section 811 of the Intelligence Authorization Act for FY 1995;

Executive orders 9397, 12829, 12968, 13467, 13587, 13526, 12333, and 10450;

Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, November 21, 2012;

Presidential Memorandum, Early Detection of Espionage and Other Intelligence Activities through Identification and Referral of Anomalies, August 23, 1996; and

Presidential Decision Directive/NSC-12, Security Awareness and Reporting of Foreign Contacts, August 5, 1993.

PURPOSE OF THE SYSTEM:

NARA established its insider threat program to consolidate and analyze insider threat information as mandated by Executive Order 13587, issued October 7, 2011. The Order requires Federal agencies to establish an insider threat detection and prevention program to ensure the security of classified networks and responsible sharing and safeguarding of classified information, consistent with appropriate protections for privacy and civil liberties. We maintain a centralized hub for insider threat analysis to (1) manually and electronically gather, integrate, review, assess, and respond to information derived from internal and external sources; (2) identify, deter, detect, and mitigate potential insider threat concerns; (3) conduct appropriate inquiries, investigations, and similar activities to resolve the concerns; and (4) manage insider threat program requirements such as tracking referrals of potential insider threats to internal and external partners and providing statistical reports.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

This system covers: (1) people who have been granted eligibility to access classified information within NARA facilities; (2) Presidential representatives granted eligibility to access classified information at Presidential libraries; and (3) members of the Public Interest Declassification Board. These individuals may include NARA civilian employees, NARA contractor personnel, and officials or employees of Federal, state, tribal, territorial, and local law enforcement organizations affiliated or working with NARA if NARA has granted them access to classified information based on an eligibility determination made by NARA or another Federal agency authorized to do so.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. We monitor user activity on all information technology networks or stand-alone systems, including use by both cleared and un-cleared employees. The Insider Threat Program may use this information to detect activity that might indicate insider threat behavior. The system includes records from this activity, including monitoring logs and insider threat analyses.

B. In addition, we may include or derive records containing information from:

(1) Responses to information requested by official questionnaires (*e.g.*, SF 86, Questionnaire for National Security Positions);

(2) Information on foreign contacts and activities; association records; information on loyalty to the United States; and other agency reports furnished to NARA or that we collect in connection with personnel security investigations, continuous evaluation for eligibility for access to classified information, and its insider threat detection program operated pursuant to Federal laws, executive orders, and NARA regulations. These records can include, but are not limited to, reports of personnel security investigations completed by investigative service providers (such as the Office of Personnel Management);

(3) Nondisclosure agreements; document control registries; courier authorization requests; derivative classification unique identifiers; requests for access to special access program (SAP) information and sensitive compartmented information (SCI); facility access records; security violation files; travel records; foreign contact reports; briefing and debriefing statements; other information and documents required in connection with personnel security adjudications; and financial disclosure filings.

(4) Records from other NARA Privacy Act systems of records. When this occurs, records from those other systems will also become part of this system of records.

(5) NARA office or program records, databases, or sources, including: incident reports; investigatory records; personnel security records; facility access records; network security records; security violations; payroll information; credit reports; travel records; foreign visitor records; foreign contact reports; financial disclosure reports; personnel records (including benefits information, performance evaluations, disciplinary files, and training records); counseling statements; equal employment opportunity complaints; outside work and activities requests; medical records; substance abuse and mental health records of individuals undergoing law enforcement action or presenting an identifiable imminent threat; personal contact records; audit data; information regarding misuse of a NARA device; information regarding unauthorized use of removable media; logs of printer, copier, and facsimile machine use; and records involving potential insider threats or activities.

(6) Records containing particularly sensitive or protected information, including information held by special access programs, law enforcement, inspector general, or other investigative sources or programs.

C. The records in this system of records may contain the following information on an individual:

(1) full name; former names and aliases; social security number; date and place of birth; mother's maiden name;

(2) prior and current security clearance, security eligibility, investigative, and adjudicative information (including information collected through continuous evaluation);

(3) current and former home and work addresses and residential history; personal and official phone numbers and email addresses; other contact information;

(4) driver's license information; vehicle identification and license plate numbers;

(5) ethnicity, gender, and race; tribal identification number or other tribal enrollment data;

(6) identifying numbers from access control passes or identification cards;

(7) employment and educational history, including degrees earned; military record information and selective service registration record;

(8) financial record information and credit reports;

(9) arrest reports and criminal history; references to illegal drug involvement and records related to drug or alcohol use;

(10) mental health records, including counseling related to use of alcohol or drugs;

(11) civil court action records;

(12) subversive activity information;

(13) outside affiliations; names of associates and references with their contact information; the name, date and place of birth, social security number, and citizenship information on spouses and cohabitants; the name, date and place of birth, citizenship, and address for dependents, and relatives; the name and marriage information for current and former spouses;

(14) citizenship information; passport information;

(15) fingerprints; hair and eye color; biometric data; height and weight; and any other individual physical or distinguishing attributes.

D. Investigation records and incident reports may include additional information on an individual, such as: photos, video, sketches, medical reports, network use records, identification badge data, facility and access control records, email, and text messages.

E. The records may also include information concerning potential insider threat activity, counterintelligence complaints, investigative referrals, results of incident investigations, case numbers, forms, nondisclosure agreements, consent forms, documents, reports, and correspondence received, generated, or maintained in the course of managing insider threat activities and conducting investigations related to potential insider threats.

F. Finally, this system contains records of inquiries the hub creates in the course of managing the Insider Threat Program. An inquiry record is akin to a case file on a possible insider threat, and may contain any of the information described above, in addition to investigatory records such as interview notes, analysis of the potential threat, voluntary statements to investigators, and similar documents.

RECORD SOURCE CATEGORIES:

We may obtain or derive information in the system from:

(1) NARA office and program officials, employees, contractors, and other individuals associated with or representing NARA;

(2) relevant NARA and contractor records, databases, and files, including: personnel security files, human resources files, facility access records, telephone usage records, user

activity monitoring information, Office of the Chief Information Officer and information assurance files, Inspector General records, security incident or violation files, network security records, investigatory records, visitor records, travel records, foreign visitor or contact reports, and financial disclosure reports;

(3) other NARA Privacy Act systems of records, which include: NARA 8: Restricted and Classified Records Access Authorization Files; NARA 11: Credentials and Passes; NARA 12: Emergency Notification Files and Employee Contact Information; NARA 14: Payroll, Attendance, Leave, Retirement, Benefits, and Electronic Reporting System Records; NARA 17: Grievance Records; NARA 18: General Law Files; NARA 19: Workers' Compensation Case Files; NARA 22: Employee-Related Files; NARA 23: Office of Inspector General Investigative Case Files; NARA 24: Personnel Security Files; NARA 27: Contracting Officer and Contracting Officer's Representative (COR) Designation Files; NARA 28: Tort and Employee Claim Files; NARA 30: Garnishment Files; NARA 32: Alternate Dispute Resolution Files; NARA 34: Agency Ethics Program Files; and NARA 43: Internal Collaboration Network (ICN);

(4) responses to information requested by official questionnaires (*e.g.*, SF 86, Questionnaire for National Security Positions);

(5) external sources including security databases and files; officials and records from other Federal, tribal, territorial, state, and local government organizations; special access programs, law enforcement, inspector general, or other investigative sources or programs; and other agency reports furnished to NARA or that we collect in connection with personnel security

investigations, continuous evaluation for eligibility for access to classified information, and its insider threat detection program; and

(6) publicly available information.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside NARA as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

(1) to the Executive Office of the President in response to an inquiry from that office made at the request of the subject of a record or a third party on that person's behalf to the extent the records have not been exempted from disclosure pursuant to 5 U.S.C. 552a(j)(2) and (k)(2);

(2) to an official of another Federal agency to provide information the agency needs to perform official duties related to reconciling or reconstructing data files or to enable that agency to respond to an inquiry by the individual to whom the record pertains;

(3) to state, local, and tribal governments to provide information in response to a court order or litigation discovery requests;

(4) to the Office of Management and Budget during legislative coordination and clearance as mandated by OMB Circular A-19;

(5) to the Department of the Treasury to recover debts owed to the United States;

(6) to the Department of Justice, the Federal Bureau of Investigation, the Department of Homeland Security, and other Federal, state and local law enforcement agencies to refer potential insider threats to them and exchange information on insider threat activity;

(7) to any criminal, civil, or regulatory authority (whether Federal, state, territorial, local, or tribal) to provide background search information on individuals for legally authorized purposes, including but not limited to background checks on individuals residing in a home with a minor or individuals seeking employment opportunities requiring background checks;

(8) to appropriate agencies, entities, and people when (1) we suspect or confirm that there has been a breach of the system of records, (2) we determine that, as a result of the suspected or confirmed breach, there is a risk of harm to individuals, NARA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and people is reasonably necessary to assist our efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm;

(9) to another Federal agency or Federal entity, when we determine that information from this system of records is reasonably necessary to assist the recipient agency or entity to (1) respond to a suspected or confirmed breach or (2) prevent, minimize, or remedy the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach; and

(10) routine uses A, B, C, D, E, F, and G listed in Appendix A (78 FR 77255, 77287) also apply to this system.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Paper and electronic records

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Staff may retrieve information in these records by the employee's name, social security number, by search, or by any available field or metadata element recorded in the system.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

NARA insider threat program records are unscheduled records; NARA therefore retains them until the Archivist of the United States approves dispositions for them. We anticipate a General Records Schedule item for Insider Threat Records will be issued for Government-wide use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

During normal hours of operation, we maintain paper records in areas accessible only by authorized NARA personnel. Authorized NARA personnel access electronic records via password-protected workstations located in attended offices or through a secure remote access network. After hours, buildings have security guards or secured doors, and electronic surveillance equipment monitors all entrances.

Access to records containing particularly sensitive or protected information, including information from special access programs, law enforcement, inspector general, or other investigative sources or programs, requires additional approval by the senior NARA official responsible for managing and overseeing the program.

RECORDS ACCESS PROCEDURES:

People who wish to access their records should submit a request in writing to the NARA Privacy Act Officer at the address listed in Appendix B. However, we exempt portions of this system from the access procedures of the Privacy Act, pursuant to sections (j)(2) and (k)(2).

CONTESTING RECORDS PROCEDURES:

NARA's rules for contesting the contents of your records and appealing initial determinations are in 36 CFR Part 1202. However, we exempt portions of this system from the amendment procedures of the Privacy Act, pursuant to sections (j)(2) and (k)(2).

NOTIFICATION PROCEDURES:

People inquiring about their records should notify the NARA Privacy Act Officer at the address listed in Appendix B. However, we exempt portions of this system from the notification procedures of the Privacy Act, pursuant to sections (j)(2) and (k)(2).

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

This system contains classified and unclassified intelligence and law enforcement investigatory records related to counterintelligence and insider threat activities that are **e**xempt from certain provisions of the Privacy Act; specifically, 5 U.S.C. 552a (k)(2). Pursuant to subsections (j)(2) and (k)(2), we exempt portions of this system from the following subsections of the Privacy Act: (c)(3), (d), (e)(1) and (e)(4)(G) and (H), and (f). In accordance with 5 U.S.C. 553(b), (c), and (e), NARA has promulgated Regulations Implementing the Privacy Act of 1974, at 36 CFR 1202.92, that establish these exemptions.

APPENDIX B

Records inquiries and requests:

To inquire about your records or to gain access to your records, you should submit your request in writing to: NARA Privacy Act Officer; Office of the General Counsel (NGC); National Archives and Records Administration; 8601 Adelphi Road, Room 3110; College Park, MD 20740-6001.

System managers:

If the system manager is the **Chief Human Capital Officer**, the business address is: Office of Human Capital; National Archives and Records Administration; 8601 Adelphi Road, Room 1200; College Park, MD 20740-6001; telephone 301.837.1981.

If the system manager is the **Chief Information Officer**, the business address is: Office of Information Services; National Archives and Records Administration; 8601 Adelphi Road, Room 4400; College Park, MD 20740-6001; telephone 301.837.1583.

If the system manager is the **Chief Innovation Officer**, the business address is: Office of Innovation; National Archives and Records Administration; 8601 Adelphi Road, Room 3200; College Park, MD 20740-6001; telephone 301.837.2029.

If the system manager is the **Chief Operating Officer**, the business address is: Office of the Chief Operating Officer; National Archives and Records Administration; 8601 Adelphi Road, Room 4200; College Park, MD 20740-6001; telephone 301.837.0643.

If the system manager is the **Chief Records Officer**, the business address is: Office of the Chief Records Officer; National Archives and Records Administration; 8601 Adelphi Road, Room 2100; College Park, MD 20740; telephone 301.837.1539.

If the system manager is the **Chief Strategy and Communications Officer or the Chief Management and Administration Officer**, the business address is: Office of Management and Administration; National Archives and Records Administration; 8601 Adelphi Road, Room 5200; College Park, MD 20740-6001; telephone 301.837.1733.

If the system manager is the **Chief of Communications and Marketing or the Chief of Staff**, the business address is: Office of the Chief of Staff; National Archives and Records Administration; 8601 Adelphi Road, Room 4200; College Park, MD 20740-6001; telephone 202.357.7458.

If the system manager is the **Designated Agency Ethics Official**, the business address is: Office of the General Counsel; National Archives and Records Administration; 8601 Adelphi Road, Room 3110; College Park, MD 20740-6001; telephone 301.837.3026.

If the system manager is the **Director, National Personnel Records Center**, the business address is: National Personnel Records Center, 1 Archives Drive, St. Louis, MO 63138; telephone 314.801.0587.

If the system manager is the **director of an individual Presidential library**, the business address is the relevant Presidential library:

George Bush Library (41), 1000 George Bush Drive West; College Station, TX 77845; telephone 979.691.4001

George W. Bush Library (43), 2943 SMU Boulevard; Dallas, TX 75205; telephone 214.346.1680

Jimmy Carter Library, 441 Freedom Parkway; Atlanta, GA 30307-1498; telephone 404.865.7100

William J. Clinton Library, 1200 President Clinton Avenue; Little Rock, AR 72201; telephone 501.244.2884

Dwight D. Eisenhower Library, 200 SE 4th Street; Abilene, KS 67410-2900; telephone 785.263.6739

Gerald R. Ford Library, 1000 Beal Avenue; Ann Arbor, MI 48109-2114; telephone 734.205.0566

Herbert Hoover Library, 210 Parkside Drive; P.O. Box 488; West Branch, IA 52358-0488; telephone 319.643.6029

Lyndon B. Johnson Library, 2313 Red River Street; Austin, TX 78705-5702; telephone 512.721.0158

John F. Kennedy Library, Columbia Point; Boston, MA 02125-3398; telephone 979.691.4004

Richard Nixon Library, 1800 Yorba Linda Boulevard; Yorba Linda, CA 92886; telephone 714.983.9121

Barack Obama Library, 2500 West Golf Road; Hoffman Estates, IL 60169-1114; telephone 847.252.5714

Ronald Reagan Library, 40 Presidential Drive; Simi Valley, CA 93065-0600; telephone 805.577.4061

Franklin D. Roosevelt Library, 4079 Albany Post Road; Hyde Park, NY 12538-1999; telephone 845.486.7741

Harry S. Truman Library, 500 West U.S. Highway 24; Independence, MO 64050-1798; telephone 816.268.8210

If the system manager is the **Director, Office of Equal Employment Opportunity**, the business address is: Office of Equal Employment Opportunity; National Archives and Records Administration; 8601 Adelphi Road, Room 3310; College Park, MD 20740-6001; telephone 301.837.0939.

If the system manager is the **Director of the Center for Legislative Archives**, the business address is: The Center for Legislative Archives; National Archives and Records Administration; 700 Pennsylvania Ave., NW; Washington, DC 20408-0001; telephone 202.357.5376.

If the system manager is the **Director of the Federal Register**, the business address is: Office of the Federal Register; National Archives and Records Administration; 800 North Capitol Street, NW; Washington, DC 20002; telephone 202.741.6100.

If the system manager is the **Director of the Office of Presidential Libraries**, the business address is the Office of Presidential Libraries; National Archives and Records Administration; 8601 Adelphi Road, Room 2200; College Park, MD 20740-6001; telephone 202.357.1662.

If the system manager is the **Director of the Presidential Materials Division**, the business address is: Presidential Materials Division; National Archives and Records Administration; 700 Pennsylvania Ave., NW, Room 104; Washington, DC 20408-0001; telephone 202.357.5144.

If the system manager is the **Director of the Washington National Records Center**, the business address is: Washington National Records Center; National Archives and Records Administration; 4205 Suitland Road; Suitland, MD 20746-8001; telephone 301.778.1553.

If the system manager is the **Executive Director of the National Historical Publications and Records Commission**, the business address is: National Historical Publications and Records Commission; National Archives and Records Administration; 700 Pennsylvania Avenue, NW, Room 114; Washington, DC 20408-0001; telephone 202.357.5263.

If the system manager is the **Executive for Agency Services**, the business address is: Office of Agency Services; National Archives and Records Administration; 8601 Adelphi Road, Room 3600; College Park, MD 20740-6001; telephone 301.837.3064.

If the system manager is the **Executive for Business Support Services**, the business address is: Office of Business Support Services; National Archives and Records Administration; 8601 Adelphi Road, Room 5100; College Park, MD 20740-6001; telephone 301.837.1719.

If the system manager is the **Executive for Information Services**, the business address is: Office of Information Services; National Archives and Records Administration; 8601 Adelphi Road, Room 4400; College Park, MD 20740-6001; telephone 301.837.1583.

If the system manager is the **Executive for Legislative Archives, Presidential Libraries, and Museum Services**, the business address is the Office of Legislative Archives, Presidential

Libraries, and Museum Services; National Archives and Records Administration; 700 Pennsylvania Avenue, NW, Room 104; Washington, DC 20408-0001; telephone 202.357.5472.

If the system manager is the **Executive for Research Services**, the business address is: Office of Research Services; National Archives and Records Administration; 8601 Adelphi Road, Room 3400; College Park, MD 20740-6001; telephone 301.837.3110.

If the system manager is the **General Counsel**, the business address is: Office of the General Counsel; National Archives and Records Administration; 8601 Adelphi Road, Room 3110; College Park, MD 20740-6001; telephone 301.837.3026.

If the system manager is the **Inspector General**, the business address is: Office of the Inspector General; National Archives and Records Administration; 8601 Adelphi Road, Room 1300; College Park, MD 20740-6001; telephone 301.837.3000.

[FR Doc. 2018-21072 Filed: 9/26/2018 8:45 am; Publication Date: 9/27/2018]